

**UNITED STATES DISTRICT COURT**  
for the  
Eastern District of Pennsylvania

United States of America  
v.

MARK GARAGOZZO

Case No.

20-MJ-1513

*Defendant(s)*

**CRIMINAL COMPLAINT**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of see attached affidavit in the county of Montgomery in the  
Eastern District of Pennsylvania, the defendant(s) violated:

*Code Section*

*Offense Description*

18 U.S.C Sections 2252(a)(4)(B),  
2252(b)(2)

Possession of Child Pornography

This criminal complaint is based on these facts:

See Attachment A

☒ Continued on the attached sheet.

*/s/ Richard Cerminaro*

*Complainant's signature*

Richard Cerminaro, Special Agent

*Printed name and title*

Sworn to before me and signed in my presence.

Date: 09/11/2020

*/s/ Lynne A. Sitarski*

*Judge's signature*

City and state: Philadelphia, Pennsylvania

Hon. Lynne A. Sitarski, Magistrate Judge

*Printed name and title*

**AFFIDAVIT OF PROBABLE CAUSE**

**Mag. No. 20-MJ-1513**

Your Affiant, Richard Cerminaro, a Special Agent with the United States Department of Homeland Security, being duly sworn, deposes and states as follows:

1. Your Affiant is a Special Agent employed by the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), assigned to the Office of the Special Agent in Charge, Philadelphia, Pennsylvania. As an HSI Special Agent, I have experience in conducting criminal investigations as it pertains to violations of Title 8, Title 18, and Title 21 of the United States Code. I am currently assigned to the HSI Philadelphia Child Exploitation and Human Trafficking unit where I investigate cases involving the sexual exploitation of minor children, the production, distribution, receipt, and possession of child exploitation materials, the coercion and enticement of minors for sexual activity, persons that travel for illicit sexual conduct, and sex trafficking by force, fraud, or coercion. I have received training in the field of child sexual abuse as well as the use of the Internet by sexual offenders to seduce, entice, and gain access to children for the purposes of sexual exploitation.

2. All information contained in this affidavit is based either on my personal knowledge or the knowledge of other law enforcement officers and agents involved with this investigation. Because this affidavit is being submitted for the limited purpose of securing an arrest warrant; I have not included each and every fact known to this investigation.

3. As will be shown below, there is probable cause to believe that Mark GARAGOZZO has committed violations of 18 U.S.C. Sections 2252(a)(4)(B) and 2252(b)(2), possession of child pornography.

**BACKGROUND OF THE INVESTIGATION**

4. In August 2020, Your Affiant was contacted about a criminal investigation being conducted by the Burlington County Prosecutor's Office ("BCPO") in New Jersey. Your Affiant learned that BCPO detectives had received Cyber Tipline reports from the National Center for Missing and Exploited Children ("NCMEC").

5. NCMEC Cybertip #59703415 detailed that on or about November 16, 2019 at approximately 13:15:28 UTC, Microsoft reported that user ID# 3000024d2168f uploaded files of child sexual abuse material ("CSAM") to Microsoft OneDrive cloud storage from Internet Protocol (IP) address 73.112.139.43. Your Affiant reviewed the NCMEC Cybertip which included the following image described below. Based on your Affiant's training and experience, the image file meets the definition of CSAM under 18 United States Code, Section 2256.

*a. File Name: ad30bf67-1ba2-4c33-9e47-6a1a58adb870.jpg*

*A pre-pubescent girl with brown hair, lying on her back, wearing an open pink robe, inserting her fingers into her vagina. The pre-pubescent girl has no visible pubic hair.*

6. NCMEC Cybertip #59677837 detailed that on or about November 16, 2019 beginning at approximately 13:15 UTC, Microsoft reported that user ID# 3000024d2168f uploaded files of CSAM to Microsoft OneDrive cloud storage from IP address 73.112.139.43. Your Affiant reviewed the NCMEC Cybertip which included the following images described below. Based on your Affiant's training and experience, the files meet the definition of CSAM under 18 United States Code, Section 2256.

*a. File Name: 09c164dc-2b13-471b-9511-92ed6de64858.jpg*

*A pre-pubescent girl, naked from the waist down, lying on her side on a pink cover. The girl's legs are spread apart exposing her vagina while a second, clothed minor girl is holding her vagina open with her hands. The pre-pubescent girl has no visible pubic hair.*

***b. File Name: 6f132ab6-0b7d-4c44-8ff7-47c5ccdb0e8e.jpg***

***A pre-pubescent girl, naked, lying on her back. The girl is bound with rope by her wrists and ankles. Her arms and legs are spread apart and what appears to be an adult male wearing blue pants is inserting an object into her vagina. This short looping video shows the object being removed and reinserted. The pre-pubescent child has no visible pubic hair.***

***c. File Name: b0ba5e09-194f-47f9-a747e6a78aa8.jpg***

***A pre-pubescent girl, naked, lying on her back on a pink cover with white dots and stars. The girl's legs are spread open exposing her vagina. A pink object is inserted into the pre-pubescent's child's vagina. The pre-pubescent girl has no visible pubic hair and appears to be approximately 3-5 years of age.***

7. A search warrant was obtained for the Microsoft OneDrive account identified by user ID# 3000024d2168f, which revealed multiple files of CSAM. A log file provided by Microsoft shows that Samsung SM-G975U and Samsung SM-N976V electronic devices were both used to access the Microsoft OneDrive user ID# 3000024d2168F account. Additionally, the email address provided by the user at the creation of said Microsoft OneDrive account was kellyrobinson0722@gmail.com.

8. Investigators served a search warrant to Google for the kellyrobinson0722@gmail.com account. The kellyrobinson0722@gmail.com account revealed Google Location History global positioning system (GPS) activity logs of an associated electronic device. The GPS data showed multiple locations in New Jersey and Pennsylvania that were associated with Verizon retail stores. Additionally, the GPS data showed activity at the 500 building of Camelot Court and 20 Walnut Street, Ambler, Pennsylvania. The kellyrobinson0722@gmail.com account also revealed multiple IP addresses associated with account activity. Of particular note were the IP addresses 2600:1001:b025:e26a:c4eb:ce8c:3f25:4cf0<sup>1</sup>

---

<sup>1</sup> The described IP address is referred to as an IPv6 internet protocol address. There are currently two types of internet protocols, IPv4 and IPv6. IPv4 addresses are commonly identified by a numeric dot-decimal notation. IPv6 addresses are commonly identified by a string of alpha-numeric hexadecimal notation. IPv6 was created, in essence, to be faster, more secure, and a more efficient means of data-device connections.

(determined by investigators to be a Verizon IP address) and 73.112.139.43 (the Comcast IP address described above used to upload CSAM that generated the CyberTips). Additionally, the account listed a recovery e-mail address as Presleykudgis@gmail.com.

9. On or about March 27, 2020, BCPO investigators served a State of New Jersey Superior Court Communications Data Warrant to Google LLC for the account presleykudgis@gmail.com. After receiving and reviewing the returned data associated with the account, investigators found an associated IP address of 73.112.81.14, the same IP address used to upload CSAM material to the Microsoft OneDrive account described above. Further review of the Google data return revealed a Samsung SM-G955U identified as a Samsung Galaxy S8+ and Samsung SM-N976V identified as a Samsung Note 10 to be associated with Presleykudgis@gmail.com.

10. Further review of the kellyrobinson0722@gmail.com account Google account revealed correspondence between kellyrobinson0722@gmail.com and the email address elintrepido\_2222@hotmail.com. Content of the conversations detailed an exchange of currency for illegal CSAM (child pornography). Elintrepido\_2222@hotmail.com referenced child pornography in the correspondence as “cp” and advised the prospective purchaser, kellyrobinson0722@gmail.com, that he was willing to sell him 200 gb of “cp” for \$50.00. Kellyrobinson0722@gmail.com was instructed to utilize Paypal as the method of payment to transfer funds to elintrepido\_2222@hotmail.com. An email followed which detailed a completed Paypal transaction for the \$50 amount specified. In your affiant’s training and experience, I know the abbreviation “cp” to be indicative of CSAM or “child pornography.” Additionally, I know that subjects involved in these types of complex cyber-crimes will frequently use digital transactions and fake email accounts in an attempt to obfuscate their illicit conduct and to evade detection and identification by law enforcement.

11. An additional email correspondence dated, January 27, 2020 at 9:59 PM between elintrepido\_2222@hotmail.com and kellyrobinson0722@gmail.com contained the following:

*“Hello friend, i have 60 gb of videos cp only of penetration for sell to 35 dollars paid by paypal”*

12. Subsequent to the email exchange with elintrepido\_2222@hotmail.com, kellyrobinson0722@gmail.com thereafter received several URL links, over multiple transactions. The links were associated with encrypted Mega Limited (also known as Mega.nz) cloud data storage accounts. The company, Mega.nz, is a cloud-based data storage electronic service provider which utilizes end-to-end encryption. Your affiant knows, through training and experience, that Mega.nz is often used by persons involved in child exploitation activities and other cyber-crimes to store, share, and/or transmit illicit digital files due to its high level of anonymity and the protection of potential evidentiary data afforded by its encryption. Mega.nz accounts and URLs can be accessed from computers, smart phones, or tablet devices connected to the internet.

13. On or about March 24, 2020, BCPO served a State of New Jersey Superior Court search warrant to Mega.nz for information and/or files linked to kellyrobinson0722@gmail.com. Pursuant to the search warrant, Mega.nz provided a data return. A review of the Mega.nz links received by kellyrobinson0722@gmail.com revealed approximately 3,000 image files and 5,000 video files of CSAM.

14. On or about April 10, 2020, a subpoena issued by BCPO to Google Payment, Inc for the account kellyrobinson0722@gmail.com revealed the following information:

Kelly Robinson  
107 Ellis Road 3  
Willow Grove  
PA 19090 US  
Account Name: kellyrobinson0722@gmail.com  
Telephone # 6096007726  
IP Address: 2600:1001:b025:e26a:c4eb:ce8c:3f25:4cf0

15. A subpoena issued by BCPO to Verizon revealed that the Verizon IPv6 address

2600:1001:b025:e26a:c4eb:ce8c:3f25:4cf0 in the Google Payment information listed in the above paragraph was registered to: ABC Phones dba "Victra," 8510 Colonnade Center Drive Raleigh, NC 27615. Additional information provided by Verizon revealed that the IPv6 address was linked to IP address 173.72.102.140, registered to Byron Henderson, 11 Schalks Crossing Road Suite 613 Plainsboro, NJ 08536. This location was identified as the Verizon Wireless Authorized Retailer, ABC Phones of NC dba "Victra." Verizon identified the telephone numbers 609-218-7589 and 609-331-0785 as being associated with this account.

16. On or about March 26, 2020, a subpoena issued by BCPO to Verizon Wireless revealed that the telephone numbers 609-218-7589 and 609-331-0785 were subscribed to Mark GARAGOZZO, 20 Walnut Street, Ambler, PA. Furthermore, 609-218-7589 was identified by Verizon as IMEI: 357959101616601, brand/model Samsung SM-G975U and 609-331-0785 as IMEI: 358645100663269, a brand/model Samsung SM-N976V. These two device make/models were reported by Microsoft as having accessed the Microsoft OneDrive account ID# 3000024d2168f.

17. On or about June 29, 2020, BCPO investigators received additional records from Google LLC related to the Google account kellyrobinson0722@gmail.com which revealed that the Samsung SM-N976V, IMEI: 358645100663269 was linked to the following Google user accounts: kellyrobinson0722@gmail.com, mynotapplephones@gmail.com, markg.mbkvisionentertainment@gmail.com, markgaragozzo.yourwireless@gmail.com, markgaragozzo1@gmail.com, markg.verizon@gmail.com, kellyrobinson0722@gmail.com, mark.dgozzo@gmail.com, marc.garagozzo@gmail.com, Markgaragozzo020289@gmail.com, presleykudgis@gmail.com, markgaragozzo10133333@gmail.com, mynvidiashieldtvemail@gmail.com, markgaragozzo101311@gmail.com, markg101311@gmail.com.

18. A search of law enforcement indices revealed Mark G. GARAGOZZO with DOB: 02/02/1989, SSN: ###-##-0953 (known to your Affiant), FBI# 909883TC6. A State of New Jersey criminal history revealed that GARAGOZZO was convicted in 2007 of Endangering the Welfare of Children- Possession/View Child Pornography, in violation of New Jersey Criminal Code, Section 2C:24-4B(5)(B). In 2010, GARAGOZZO was convicted of Theft by Deception and Credit Card Crime, in violation of New Jersey Criminal Code, Section 2C:20-4A.

19. A search of the New Jersey Department of Labor revealed that GARAGOZZO is employed by ABC Phones of NC.

20. An open source indices search of GARAGOZZO revealed the current reported address of 20 Walnut Street, Ambler, PA. GARAGOZZO's listed previous addresses included 107 Ellis Road, Willow Grove, PA 19090. GARAGOZZO reported the telephone numbers 609-218-7589 and 609-331-0785.

21. On August 28, 2020 at approximately 08:45 AM, your Affiant conducted surveillance at 20 Walnut Street Ambler, PA. At approximately 09:25 AM, your Affiant observed a white male matching GARAGOZZO's description enter a dark colored Volkswagen Tiguan with New Jersey License Plate G19-KAN and depart 20 Walnut Street Ambler, PA. Your Affiant observed the driver of said vehicle and identified the driver as GARAGOZZO.

### **THE SEARCH WARRANT**

22. On September 11, 2020, at approximately 07:30 AM, your Affiant along with additional law enforcement investigators executed a search warrant at 20 Walnut Street Ambler, PA 19002 for that property and for the person of Mark GARAGOZZO.<sup>2</sup> GARAGOZZO was encountered inside the residence and agreed to be interviewed by your Affiant and other

---

<sup>2</sup> In addition to the instant federal charges, BCPO has also charged GARAGOZZO with child exploitation offenses in New Jersey in Complaint No. 0308-W-2020-000378, and an active arrest warrant was executed at the same time that the EDPA search warrants were executed.



investigators. At approximately 07:44 AM, GARAGOZZO was provided and read his Miranda Statement of Rights, to which he agreed to waive his rights and answer any questions.

GARAGOZZO was not handcuffed during this interview and was provided refreshments upon his request. The interview was audio and video recorded.

23. GARAGOZZO stated that he is familiar with the email address kellyrobinson0722@gmail.com and that he has operated this email account for the purposes of creating and operating his online accounts, which he admitted contained CSAM. GARAGOZZO admitted that he accessed multiple Mega.nz URLs which he admitted contained CSAM of varying ages. GARAGOZZO also admitted to utilizing a Microsoft OneDrive account, which he used to sync his cellular telephone. He admitted the OneDrive account contained CSAM.

24. GARAGOZZO stated that he currently utilizes a Samsung Galaxy Note 10 smart phone with telephone number 609-331-0785. GARGOZZO provided his passcode for that Samsung GALAXY Note 10 cell phone, which was located in his bedroom within 20 Walnut Street, Ambler, PA.

25. A preview of GARAGOZZO's Samsung Galaxy Note 10 cell phone revealed a "Downloads" folder titled Mega downloads. This folder showed an approximate access date of August 19, 2020; however, the folder was found to be empty. An encrypted application titled "Secure Folder" was also located on GARAGOZZO's cell phone. This Secured Folder was password protected, which was found to be different from the passcode he provided to unlock his Samsung Galaxy Note 10 cell phone. GARAGOZZO provided the passcode to this secured folder. Upon review, this Secured Folder was found to contain multiple subfolders containing image and video files. An album titled "Album 1" was found to contain image and video files depicting CSAM. Based on your Affiant's training and experience, the following image and video files meet the definition of CSAM under 18 United States Code, Section 2256 and were observed by this

Affiant:

a. *Image file titled 307.jpg dated Sept. 4, 2020 at 2:28AM*

*A pre-pubescent girl naked from the waist down wearing a gray T-Shirt and glasses, seated on an orange colored chair with her legs spread while exposing her vagina in a lewd and lascivious manner. The age of the pre-pubescent girl appears to be approximately 8-10 years of age. The pre-pubescent girl has no visible pubic hair.*

b. *Video file titled VID-20140907-WA0001.mp4 dated Sept. 4, 2020 at 2:29AM*

*A pre-pubescent girl wearing a blue dress naked from the waist down. Throughout the video the pre-pubescent girl is positioned on her hands and knees and her back on top of a bed. The pre-pubescent girl is being anally and vaginally penetrated by an adult male. The age of the pre-pubescent girl appears to be approximately 6-8 years of age. The pre-pubescent girl has no visible pubic hair.*

c. *Image file titled 126714898\_1567825160.jpg dated Sept. 4, 2020 at 2:29 AM*

*A pre-pubescent girl naked lying on a dark colored blanket and a pink pillow with cartoon kitty and balloons, with her legs spread open exposing her vagina in a lewd and lascivious manner. A clear liquid suspected of being semen can be seen on her stomach area. The age of the pre-pubescent girl appears to be approximately 8-10 years of age. The pre-pubescent girl has no visible pubic hair.*

26. The Samsung Galaxy Note 10 cell phone on which the above described files were found is capable of accessing the internet, and matches the make/model of the device used to access the Microsoft OneDrive account. It was not manufactured in Pennsylvania.

**CONCLUSION**

27. Based on the aforementioned factual information, your Affiant respectfully submits that there is probable cause to believe that Mark GARAGOZZO has violated 18 U.S.C. Section 2252(a)(4)(B), possession of child pornography.

28. In consideration of the foregoing, your Affiant respectfully requests that this Court issue a warrant for the arrest of Mark GARAGOZZO.

Respectfully submitted,

/s/ Richard Cerminaro

Richard Cerminaro  
Special Agent, HSI

Subscribed and sworn before me  
this 11<sup>th</sup> day of September, 2020.

/s/ Lynne A. Sitarski

HONORABLE LYNNE A. SITARSKI  
United States Magistrate Judge